Home Office

AUTHORITY: The Secretary of State for the Home Department

Volume 3

Schedule R

IT System Requirements – Part 1 & 2

Travel Services

Volume	Title
Main Contract	Services Agreement
Schedules to Volume 3	SCHEDULE A Insurance
	SCHEDULE B Mobilisation & Permit to Operate
	SCHEDULE C Interim State
	SCHEDULE D Service Specification Part 1: Service Specification Part 2: Service Provider's Response
	SCHEDULE E Form of Parent Company Guarantee
	SCHEDULE F Payment Mechanism
	SCHEDULE G Performance Evaluation & Service Unavailability
	SCHEDULE H Innovation and Partnering Agreement
	SCHEDULE I Commercially Sensitive Information
	SCHEDULE J Dispute Resolution Procedure
	SCHEDULE K Permitted Sub-contractors and Sub-contracts
	SCHEDULE L Change Control Procedures
	SCHEDULE M Named Representatives
	SCHEDULE N Demobilisation
	SCHEDULE O Service Improvement
	SCHEDULE P Financial Distress
	SCHEDULE Q Financial Reports & Audit Rights
	SCHEDULE R IT Systems Requirement **Part 1: IT Systems Requirement** **Part 2: IT Service Management Requirements & applicable annexes** Part 3: Service Provider's Response
	SCHEDULE S Contract Management
Volume 4	Data Room

CONTENTS

AUTHORITY: THE SECRETARY OF STATE FOR THE HOME DEPARTMENT 1
SCHEDULE R 1
IT SYSTEM REQUIREMENTS – PART 1 & 2 1
TRAVEL SERVICES 1
PART 1 7
1. INTRODUCTION 7
1.1 General 7
2. TS FUNCTIONAL REQUIREMENTS 8
2.1 Flight Determination 8
2.2 Data exchange 9
2.3 Travel Information Guide (TIG) 10
3. TS NON-FUNCTIONAL REQUIREMENTS 11
3.1 Access Management -1 11
3.2 Access Management -2 11
3.3 Availability Management -3 11
3.4 Application-1 11
3.5 Application-2 11
3.6 Application-3 11
3.7 Application-4 11
3.8 Application-5 12
3.9 Application-6 12
3.10 Security Management-1 12
3.11 Security Management -2 12
3.12 Security Management -3 12
3.13 Security Management -4 12
3.14 Security Management -5 13
3.15 Security Management -6 13
3.16 Security Management -7 13
3.17 Security Management -8 13
3.18 Security Management -9 13
3.19 Security Management-10 13
3.20 Security Management-11 14
3.21 Security Management-12 14
3.22 Security Management-13 14
3.23 Security Management-14 15
3.24 Technical Hosting & Maintenance-1 15
3.25 Technical Hosting & Maintenance-2 15
3.26 Incident Management, and other supporting Service Management Processes 15
3.27 Infrastructure 15
PART 2 15
1. THE SERVICE MANAGEMENT POLICIES REFERENCED 16
2. GENERIC SERVICE OBLIGATIONS 17
Please refer to Appendix C for Balanced Scorecard Measures 38
4. APPENDIX A – MESSAGING AND DATA FLOW 39
4.1 Message 1: Escort quote request 40
4.2 Message 2: Escort quote response 41
4.3 Message 3: Travel quote request 42
4.4 Message 4: Travel quote response 42
4.5 Message 5: Escort booking request 43
4.6 Message 6: Escort confirmation response 43
4.7 Message 7: Travel booking request 44

4.8 Message 8: Travel booking response 44
4.9 Message 9: Escort amendment 45
4.10 Message 10: Escort update 46
4.11 Message 11: Travel amendment 47
4.12 Message 12: Travel update 47
4.13 Message 13: Travel cancellation 49
4.14 Message 14: Escort cancellation 49
APPENDIX B – HUB REQUIREMENTS 50
4.15 Service Access (Authority System) 50
4.16 Roles and Responsibilities 50
4.17 Travel Service business rule management 50
4.18 Travel Request service approach 50
4.19 Search Function 51
4.20 Travel Amendments and Cancellations 51
4.21 Booking Status 51
4.22 Duplicate bookings 51
APPENDIX C 52
Balanced Scorecard Measures 52
APPENDIX D 53

DEFINITIONS AND ABBREVIATIONS

The following is a list of the key definitions and abbreviations used throughout this document.

Term	Definition
Application Programme Interface (API)	Set of functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or other service.
Assisted Departures Team (ADT)	Assisted Departures Team (ADT). A team that manages a scheme which enables persons choosing to leave the UK voluntarily via the Assisted Departure Scheme. This scheme is supported by the Services delivered under the Contract.
Authority	This refers to the contracting Authority which is the Secretary of State for the Home Department
Best Value Process	The process detailed in Schedule D (Service Specification) - *Annex D*, by which the Authority shall determine the best value removal package to be booked by the Service Provider.
Broker	Means a party that functions as an intermediary between the Service Provider and the Charter Company in negotiating agreements relating the procurement of Charter Flights.
Carrier	Provider of air, sea, car or rail travel.
Charter	Means the leasing of an aircraft or other mode of transport for the specific and exclusive use of the undertaking Authority business.
Charter Provider Cancellation Event	Instances where the Service Provider or Charter Company may cancel a Charter flight, without incurring a financial deduction under the terms of this contract. Charter Provider Cancellation Events shall be strictly limited to the situations specified in paragraph 3.7.16 in Schedule D (Service Specification), which create delays/unavailability affecting the Charter Aircraft only.
Charter Company	Any Party subcontracted by the Service Provider to deliver a Charter.
Charter Programme	A list or “Charter Calendar” of one or more flights detailing destinations and dates of required Charter flights as specified by the Authority
Contract	A contract for travel Services made between the Authority and the successful Bidder for the provision of travel Services
Criminal Casework (CC)	Criminal Casework. A specific case working area within Immigration Enforcement.
DAC	Detained Asylum Casework. A specific case working area within UK Visas & Immigration (UKVI)
Escort Services	Escorting services, which include the provision of medical care to Detainees for all or part of their journey
Escort Services Provider (ESP)	The provider of Escort Services to the Authority.
E&T	Escort & Travel

Immigration Compliance and Enforcement Teams (ICE Teams)	Immigration Compliance & Enforcement team. Operational arrest teams
Escort Staff	Personnel provided by the Escort Service Provider and /or the Authority for the purposes of Escort Services
Information HUB	Home Office Information HUB, will be a tool designed and developed by the Authority. It will be the tool within which Home Officer users can access and update the information relating to an in country move or a removal request.
ITT	The Invitation to Tender for the Services.
NRC	National Removals Command. A specific case working area working within Immigration Enforcement.
Performance Data	Data collated and reported in relation to the performance of the Service
Performance Standard	A summary of the Authority's Service requirement for a particular operational requirement
Return	Means the removal of a person from the United Kingdom under immigration powers/for immigration purposes. For the purposes of the contract this term shall also cover transportation of individuals to or from the UK for any immigration purposes.
Returns Logistics Charter Team	Team responsible for the operational management and procurement of the Home Office Charter Programme
Services	The travel services to be provided by the Service Provider in accordance with the terms of the Contract.
Service Provider	The organisation selected to deliver the Travel Services – The Travel Services Provider (TSP)
Service Request	A request made by the Authority for Services defined in this Service specification
Staff	All employees, servants or agents of the successful Tenderer employed in relation to provision of the Services.
TCU	Third Country Unit
Tender	A completed submission which is to be submitted to the Authority by a Tenderer by the due date
Tender Period	The period between the issue of this ITT and the deadline set by the Authority for receipt of Tenders.
Tenderer	The organisation or consortium that is invited to submit a Tender in response to this ITT
Tenderer Party	Any employee, consultant, advisor, agent, officer or Sub-contractor (of any tier) of the Tenderer
Travel Information Guide (TIG)	An electronic document describing information for each country in respect of which Travel Services are required. This information includes acceptable routes; notification periods; operating airlines etc
Travel Services Provider (TSP)	The provider of Travel Services to the Authority.

PART 1

1. INTRODUCTION

1.1 General

1.1.1 This Part 1 of the IT System requirements for Travel Services of Schedule R sets out the Authority's Requirements in respect of the Contract. Part 2 IT Service Management sets out the responsibilities of the Service Provider for the ongoing IT service. Part 3 Service Provider's Response to this Schedule R contains the Service Provider's response or required response to IT System requirements for Travel Services set out in Part 1 & 2. The Service Provider shall provide the Services in accordance with both Parts 1 and 2 and in any instances of ambiguity or conflict this Part 1 shall take primacy.

1.1.2 Structure of this Part 1 IT System requirements for Travel Services:

- The IT System requirements consist of two parts: the Functional requirements and the Non-Functional requirements.
- The Travel Service Specification details the Authority's travel-specific requirements for the Services.

1.1.3 (Overriding obligation):

- The Service Provider shall comply with all of the requirements of the IT System Requirements Specification.

1.1.4 (Content):

a) The content of the IT Specification sets out the:

- Aims and objectives of the IT;
- Scope of the IT; and
- Service requirements;

b) Each IT requirement described within the IT System requirements outlines the Authority's minimum specific requirements in relation to the Services.

c) For each Service, the Service Provider is expected to deliver all requirements in this contract. The Authority has devised a performance regime detailed in schedule G covering key performance indicators, and other performance indicators for this contract. The Service Provider's performance in relation to the Services will be assessed on a pass or fail basis, as against the Service Specifications, and the Schedule G Performance Regime.

2. TS FUNCTIONAL REQUIREMENTS

This segment of the document defines the high level IT requirements needed for the technology components that underpin the delivery of the Travel Service that is used by operational business areas across the Home Office. Currently: Criminal Casework, National Removals Command (both detained and non-detained), Assisted Departures Team, Detained Asylum Casework, Removals Casework, ICE Teams, TCU and Border Force.

The aim of this document is to define the functional and non-functional requirements for a To-Be Travel Management system which will enable the Home Office to manage travel associated activities in a more cohesive and efficient way than is currently the case under existing arrangements.

The Home office users will manage the provision of travel and escorting related to “returnee” cases through a system called the hub. The hub will track and structure the case working to fulfil the service from request, to either completion or cancellation, including updates and amendments.

The Home Office expects bidders for the TSP to articulate how they would provide the information required by the Authority whether via an integrated interface that will be built in to the service (please see Annex D) or a web form provided by the Home Office.

The TSP solution must support the following.

- Single entry of data for Home Office staff booking public expense removals (charter, scheduled and other forms of travel).
- Exchange of data between the TSP and the ’HUB’.
- The ability for the booker to cancel bookings enabling refunds to be maximised and escorts reallocated.
- Provision of the necessary information to the Home Office ‘HUB’ to enable the Authority to track the level of refunds owed for cancelled tickets’.

2.1 Flight Determination

1. The Home Office user will send the TSP details about the returnee and their intended removal details.
2. The Travel Service Provider will identify some travel quotes.
3. The Home Office will agree with the TSP which one of the quotes is best or if a charter options (maintained by the Home Office) is preferred.
4. If a charter is chosen, this will be managed internally in the Home Office and the TSP will be informed not to proceed with a booking.
5. If one of the provided quotes represents best value, then the TSP will be informed to book a specified quote.

2.2 Data exchange

The diagram below illustrates the information exchange between the Home Office and the Travel service system for un-escorted out of country moves.

The process set out below outlines the most common scenario for unescorted travel requests. The Service Provider is to suggest how this information exchange would occur.

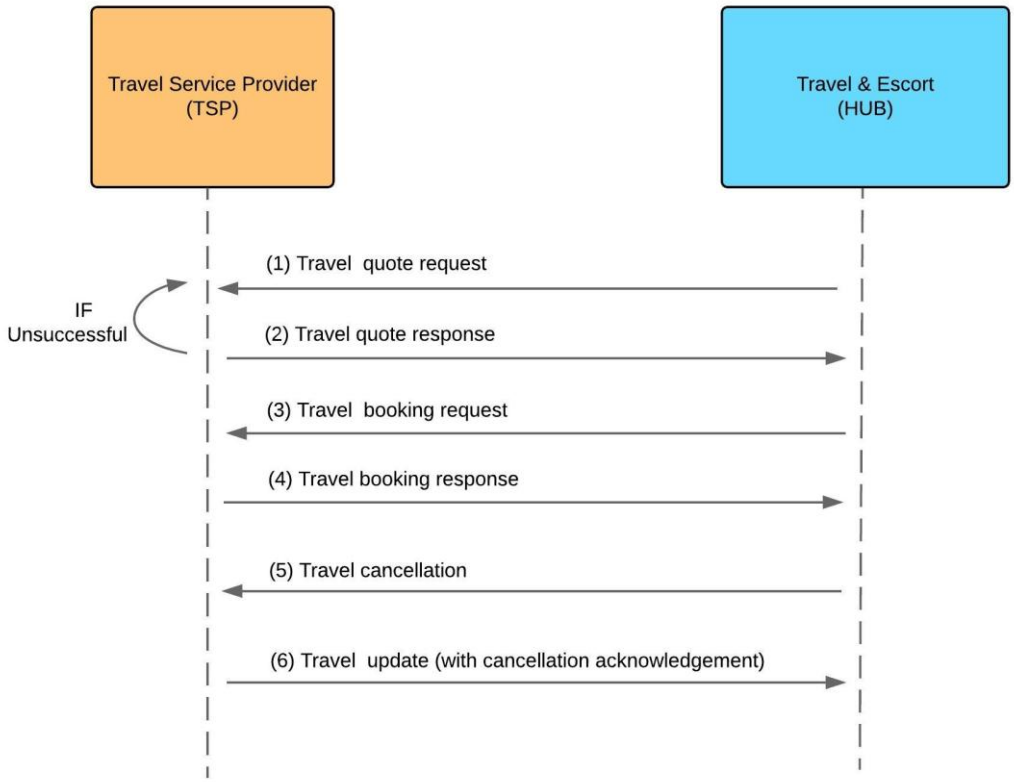


Figure 1.0

The Diagram below illustrates the electronic data exchange between the Home Office, the Travel Service and the Escort Service Provider for Escorted out-of-country moves.

The Service Provider is to suggest how this information exchange would occur.

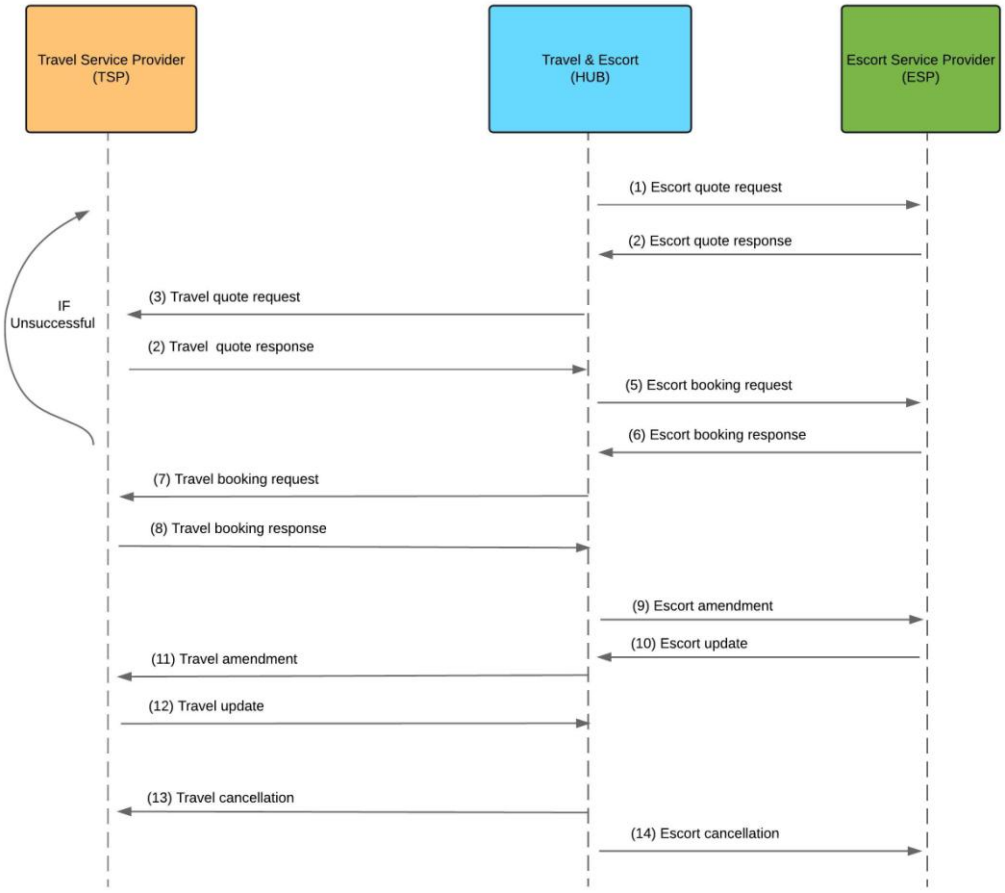


Figure 2.0

The above two scenarios show how data will be exchanged between the Home Office, Travel Service and the Escort Service Provider. It will be mandatory for the Travel Service Provider to send the data back to the ''Authority'' via either an integrated interface that will be built in to the service (please see Annex D) or a web form provided by the Home Office that approved supplier staff will be given access to so that the Home Office will avoid additional data entry.

Any requests for service and other communications from the Authority will be automated messages generated form the Home Office system (unless there is an exceptional circumstance such as an urgent request for travel). The Service Provider is to specify in their response what formats such communications are required to be in.

2.3 Travel Information Guide (TIG)

The TIG will be in an excel spread sheet which approved staff will have access to and that the Authority will update. It will be hosted on the HUB. The TIG will solely be owned by the Authority with the input of TSP who will be given administrator rights to make any updates necessary. This will help both parties to be able to make updates in a centralised way that will be more efficient and streamline.

3. TS NON-FUNCTIONAL REQUIREMENTS

3.1 Access Management -1

NFR-ID: 0001
Category: TSP
Type: Accessibility
Description: The service accreditation for the TSP must be at Official/Personal Sensitive level.

3.2 Access Management -2

NFR-ID: 0002
Category: TSP
Type: Accessibility
Description: The service is able to produce access-audit-logs which can be read by an external protective monitoring solution.

3.3 Availability Management -3

NFR-ID: 0003
Category: TSP
Type: Availability
Description: The service must be available 99.5% of time 24 x 7 x 365 (excluding agreed change outages/planned maintenance), with resiliency built into the design.

3.4 Application-1

NFR-ID: 0004
Category: TSP
Type: Application
Description: The service provider must ensure the solution adheres to the data definitions specified by the Corporate Data Model and Home Office Data Policy.

3.5 Application-2

NFR-ID: 0005
Category: TSP
Type: Application
Description: The service provider must ensure the solution enables the potential ability to encapsulate / isolate the configuration of decisions and rules affecting the execution and output of a business process from the actual process flow itself.

3.6 Application-3

NFR-ID: 0006
Category: TSP
Type: Application
Description: The service provider must ensure the solution promotes the ability to use centrally maintained reference data sets as opposed to hard-coding lists of values or maintaining reference data within individual software components

3.7 Application-4

NFR-ID: 0007
Category: TSP
Type: Application

Description: The service provider to ensure the solution employs error-handling so as to reduce to negligible, the likelihood that any operation shall result in the application itself or any COTS products, browsers, etc that use it generating an unhandled exception (e.g. System crash).

3.8 Application-5

NFR-ID: 0008
Category: TSP
Type: Application
Description: The service provider to ensure the solution design provides early alerting and well defined steps to recover from unhandled exceptions

3.9 Application-6

NFR-ID: 0009
Category: TSP
Type: Application
Description: The service provider must ensure the solution accurately presents information that is held by the solution or retrieved from external source system

3.10 Security Management-1

NFR-ID: 0011
Category: TSP
Type: Security
Description: Service Provider must ensure that Authority data is securely deleted when any defined data retention period has expired or when the Authority directs that data is no longer required or to satisfy statutory or legal obligations. The Service Provider shall ensure that Authority data is deleted in a manner which is compliant with its protective marking.

3.11 Security Management -2

NFR-ID: 0012
Category: TSP, ESP and HUB (Home Office)
Type: Security
Description: Service Providers/Architect/Developer/Business to ensure that any data that they generate is retained legally in compliance with statutory or legal obligations such as the Data Protection Act 1998.

3.12 Security Management -3

NFR-ID: 0013
Category: TSP
Type: Security
Description: Service Providers to comply with the requirements of any codes of connection, multilateral or bilateral international agreements and community or shared services security policies to which the Authority are signatories (e.g. Government Secure Intranet);

3.13 Security Management -4

NFR-ID: 0014
Category: TSP
Type: Security

Description: Users of the system must be trained in security policies, their responsibilities and consequences of breaching security rules. There should be an appropriate warning of breaches of policy at login (this is a legal requirement if the user is being monitored).

3.14 Security Management -5

NFR-ID: 0015
Category: TSP
Type: Security
Description: User access must be managed sufficiently to ensure access to sensitive information/assets is only granted to personnel with business need and appropriate clearance.

3.15 Security Management -6

NFR-ID: 0016
Category: TSP
Type: Security
Description: The Service Provider develops the system in accordance with and in such a way as to ensure Home Office Security accreditation is achievable. Service Providers will be required to deliver capabilities in accordance with the HMG Security Policy Framework (SPF) and its supporting documentation issued by organisations such as the Cabinet Office. It should be noted that certain aspects of the SPF are only available to specialist security consultants; such resource requirements should be taken into consideration.

3.16 Security Management -7

NFR-ID: 0017
Category: TSP
Type: Security
Description: Service Providers to perform risk assessments and act to mitigate the determined risks. Accreditation of systems handling Authority data will be required to be accredited before system go-live. Annual IT health-checks will also be required to ensure this accreditation is maintained.

3.17 Security Management -8

NFR-ID: 0018
Category: TSP
Type: Security
Description: Service Providers support a working relationship between security representatives and the Authorities equivalents.

3.18 Security Management -9

NFR-ID: 0019
Category: TSP
Type: Security
Description: Service Providers to ensure that there is an efficient system of reporting, recording and investigating breaches of security, which the Authority security staff can monitor, in accordance with HMG Security Policy Framework.

3.19 Security Management-10

NFR-ID: 0020
Category: TSP

Type: Security
Description: All transactions must be logged in line with the protective monitoring requirements.

1. Implementation of a PM (Protective Monitoring) solution that can automate the aggregation of audit log data, its consolidation, analysis and real time or semi-real time automated alerting. The capability/tool should cover the entire IT hosting environment for every scoped line-of-business system covering network-level, application-level and platform-level security logs/events.
2. The tool/capability should be designed in a way that enables it to integrate with multiple systems of different security classifications.
3. The monitoring use-cases should as a minimum cover:-

a) Creation/Deletion/Change of admin accounts.
b) Creation/Deletion/Change of user accounts.
c) Failed logon events that occurred successively more than 5 times within 30 minutes of each other.
d) Automated account lock-out events.
e) Accounts that is dormant for more than 3 months.
f) High severity HIPS alerts.
g) High criticality OS patch alerts.
h) Malware alerts.
i) High severity network traffic alerts across firewall boundaries.
j) Administrative access to Host OS (hypervisor).
k) Process (or service) creation/instantiation events on the guest OS.
Security log-data deletion/reset/capacity-overrun events.

3.20 Security Management-11

NFR-ID: 0021
Category: TSP
Type: Security
Description: The solution must comply with Home Office security requirements to facilitate and retain accreditation.

3.21 Security Management-12

NFR-ID: 0022
Category: TSP
Type: Security
Description: The service provider and its supply chain, relevant to the scope of the solution, must have formal certifications in accordance to one or any of the following: -

* ISAE-16 / ISAE 3402;
* ISO 27001 certifications;
* Cloud Certification Schemes such as CSA;
* Cyber Essentials PLUS certifications.

The attestations will be reviewed with the HO security operations teams prior to contract finalisation.

3.22 Security Management-13

NFR-ID: 0023
Category: TSP
Type: Security
Description: The service provider must provide documentation that describes the security architecture for their product, including authentication for html based

interfaces.

3.23 Security Management-14

NFR-ID: 0024
Category: TSP
Type: Security
Description: Service Providers to provide suitably skilled security resources in the areas of information assurance and security architectures to create detailed user stories for the design and build of any system the TSP feels they need to build to support a working relationship with equivalent resources at the Authority.

3.24 Technical Hosting & Maintenance-1

NFR-ID: 0025
Category: TSP
Type: Security
Description: All timestamps created by the solution shall either have the time zone included in the timestamp.

3.25 Technical Hosting & Maintenance-2

NFR-ID: 0026
Category: TSP
Type: Security
Description: the solution to operate according to a consistent time format. The Service Provider shall ensure that the application is developed on environments that use the London time zone (i.e. GMT+0000/BST+0100).

3.26 Incident Management, and other supporting Service Management Processes

NFR-ID: 0027
Category: TSP
Type: Incident Management
Description: Please refer to Part 2 for Incident Management

All Service Management processes should be developed in line with ITIL v3 or equivalent.

3.27 Infrastructure

NFR-ID: 0027
Category: TSP
Type: Infrastructure
Description: The location for the Service Provider data centre must be within Home Office specified Territories, i.e. within Europe with UK preferred.

PART 2

IT SERVICE MANAGEMENT

The Generic Service Obligations (GSOs) described in this guide are aligned to the ITILv3 (2011) framework.

A relevant sub-set set of IT Service Management GSOs which the Home Office apply to ensure that IT Services can be properly supported in the live environment.

The GSOs ensure the alignment of IT Service suppliers with the Authority's IT Service Management model. It should be noted that not ALL of the GSOs HAVE to be applied – service characteristics must be borne in mind and the GSOs tailored to ensure they are in context and proportionate to the service in question.

The GSO descriptions detailed within this document are broken down into each ITIL process and define the obligations and measures for suppliers to adhere to in delivering those ITIL processes to Home Office. Contracts which Home Office consider to be of high importance to its operation will typically include all of these. The number and range of GSOs required within each supplier contract depend on the criticality of the contract and the service management process they align to. Terms used in this document are defined in Home Office Policies and Procedures Definitions document. This document also includes obligations for IT Service Management Tooling Interface requirements.

Ser	GSO	Measure	Notes	GSO Ref No.	T3

Ser – a reference number
GSO – the basic supplier or contractor obligation description
Measure – how the obligation will be measured
Notes – any applicable notes that provide context or additional detail on the obligation
GSO Ref – a simple reference to the generic obligation for data analysis/tracking across supplier contracts
T3 (applicable Tier level for this ITT) – this is split into levels that describe the depth or breadth of contracted service.

Each entry has a M/S/C/W 'label' adopting the MoSCoW methodology where:

- M = Must Have,
- S = Should Have,
- C = Could Have,
- W = Won't have.

1. THE SERVICE MANAGEMENT POLICIES REFERENCED

The following life of Home Office Policies are applicable to this ITT:

- Access Management Policy
- IT Asset & Configuration Management Policy
- Capacity Management Policy
- Change Management Policy
- Event Management Policy
- Incident Management Policy
- IT Service Continuity Policy
- Knowledge Management Policy
- Problem Management Policy
- Release Management Policy
- Security Policy
- Service Desk Policy

- Service Level Management Policy
- Standards and Architecture Policy
- Supplier Management Policy

2. GENERIC SERVICE OBLIGATIONS

Ser	GSO	Measure	Notes	GSO Ref No.	T3
Access Management					
1	The Contractor shall comply with the Authority's Access Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Access Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 17	S
2	The Contractor shall, when required as a result of a Service Desk access request, provide user access to the System or Application as specified	KPI - % of Access Requests successfully completed each SMP within the specified timescales and with supporting the Authority's 99.5% target		SIAM 18	S
IT Asset and Configuration Management					
3	The Contractor shall comply with the Authority's IT Asset & Configuration Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant IT Asset & Configuration Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 61	S
4	The Contractor shall maintain an accurate and up to date Configuration Management Database (CMDB) that provides the Authority with an end-to-end pictorial view of its IT estate	Service Level - % check of Configuration Items accurately recorded in the CMDB by means of a physical check of the percentage of a minimum of 500 Configuration Items (CI) per SMP including all associated software licence checks. Target 99% are accurately recorded.	This is a Balanced Scorecard Measure	SIAM 62	S
5	The Contractor shall actively identify and inform the Authority about redundant Assets (hardware and software) to support cost reduction	KPI - Notify SIAM within 10 working days when an asset becomes redundant each SMP. Target 100%	-	SIAM 65	S
Availability Management					
6	The Contractor shall comply with the Authority's Availability Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Availability Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 77	S
7	The Contractor shall reduce the impact to the Authority's customers of failure of their IT services and systems provided	KPI - Reduce year on year the number of Working Days Lost through IT Service disruption against set targets. Standard target for availability is 99.5%	-	SIAM 78	C

8	The Contractor shall provide all information required to enable the Authority to produce end-to-end systems transaction processing measurements. E.g. time associated with processing a request for travel. Note TBC by the contractor how this will be done.	KPI - completeness and accuracy of reporting information provided within set timescales each SMP. 100% Target	-	SIAM 79	C
9	The Contractor shall connect to the Authority's IT Service Management Toolset that provides a single direction interface (as per Tooling Requirements) between the Contractor and the Authority's IT Service Management Toolset to enable the up streaming of performance and Availability Management information data in real time/near real time and by scheduled up streaming	-	The Authority will provide the Contractor with a Tooling Interface Requirements document to enable Suppliers to Interface with the Authority's IT Service Management Toolset	SIAM 80	S
10	The Contractor shall ensure Systems and Service Availability are designed to meet Home Office requirements so that the services provided meet the Authority's business needs	KPI - Contractor Service Reliability each SMP. 99.70% Target or greater KPI - Contractor Service Availability each SMP. 99.80% Target or greater	These are both Balanced Scorecard Measures	SIAM 81	S
Capacity Management					
11	The Contractor shall comply with the Authority's Capacity Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Capacity Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 89	S
12	The Contractor shall work collaboratively with the Authority and other Contractors as nominated by the Authority to provide the optimum amount of IT capacity to meet business need	-The Authority will collaborate with the contractors in making demand predictions available to assist in IT capacity management predictions and planning by the contractors	Not required if the Agreement includes a Collaboration Schedule	SIAM 90	S
13	The Contractor shall ensure that evolving business requirements are accurately assessed in order to optimise future, more cost effective, capacity demand for the Authority	KPI - No of incidents caused by a lack of adequate IT capacity. Target no more than 1 Priority 1 or 2 incidents per reporting period. The contract should report on capacity as part of the monthly service reporting.	This is a Balanced Scorecard Measure	SIAM 93	S

Change Management					
14	The Contractor shall comply with the Authority's Change Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Change Management Policies & Procedures	-	SIAM 44	S
15	The Contractor shall reduce the amount of service and business disruption and Incidents caused by Change activity	KPI - Number of and % of outages due to planned changes which have not had any effect on service availability each SMP 99% Target	-	SIAM 45	S
16	The Contractor shall provide details of all proposed and planned changes to the Authority for inclusion in the Forward Schedule of Change (FSC).	-	FSC is a SIAM product bringing together a view of all planned and proposed changes	SIAM 50	S
17	The Contractor shall use the CMDB as the Authority source of information when changes are proposed, planned and implemented and shall update the CMDB in line with IT Asset & Configuration Management policies and procedures	KPI - no more than 1% of incidents to be as result of changes impacted against incorrect details in the CMDB	-	SIAM 51	S
Event Management					
18	The Contractor shall comply with the Authority's Event Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Event Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 06	S
19	The Contractor shall raise Incidents where significant impacting events are detected	KPI - Total number of incidents that occurred and percentage of these that were triggered without a corresponding event. 0% Target	-	SIAM 08	S
Incident Management					
20	The Contractor shall comply with the Authority's Incident Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Incident Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 23	S

21	The Contractor shall improve the contracted service(s) provided to the Authority by minimising the impact of business disruption caused by Incidents	Service Level - 99.5% (minimum) Incident Resolution Severity 1, Report down to Contractors Service/site level. Target time 4 hours of incident being assigned. KPI - 99.5 % (minimum) Incident Resolution Severity 2, Report down to Contractors Service/site level. Target time of 8 hours of incident being assigned. KPI - 98% (minimum) Incident Resolution Severity 3, Report down to Contractors Service/site level. Target time of 2 working days of incident being assigned. KPI - 98% (minimum) Incident Resolution Severity 4, Report down to Contractors Service/site level. Target time of 4 working days of incident being assigned.	These are Balanced Scorecard Measures	SIAM 24	S
22	The Contractor shall improve overall Service Availability by reducing the time taken to resolve Incidents	KPI Mean Time to Resolve Incidents - demonstrable reduction in time each year from a baseline taken over 1st year of operation	-	SIAM 26	S
23	The Contractor shall ensure Incident Records are complete and up to date at all times and are linked to any other impacted areas including but not limited to Contractor's CMDB, Problems, Change Records	-Incident updates report frequency by priority level:- P1 – every 30 minutes P2 – every hour P3 – once per day P4 – once per day	-	SIAM 27	S
24	The Contractor shall perform trend analysis on Incidents assigned to the them to inform service improvements	-	-	SIAM 28	S
25	The Contractor shall connect to the Authority's IT Service Management toolset that provides a bi-directional interface between the Contractor and the Service Desk to enable information transfer in respect of Incidents if that is supported by the Home Office, if not then there must be an agreed mechanism and governance to enable information transfer in the event of an incident.	-	-	SIAM 29	S
IT Service Continuity Management					

26	The Contractor shall comply with the Authority's IT Service Continuity Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant IT Service Continuity Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 82	S
27	The Contractor shall perform IT Service Continuity Tests in accordance with the Authority's IT Service Continuity Test Programme and resolve any issues that are discovered during the Tests	KPI - Number of IT Service Continuity Tests actually performed to the agreed recovery requirements and within the timeframe expected against the number due to be carried out. 100% Target Once per year as minimum	-	SIAM 83	S
Knowledge Management					
28	The Contractor shall comply with the Authority's Knowledge Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Knowledge Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 13	S
29	The Contractor shall work with Service Design and Service Transition to provide new and updated Knowledge artefacts and retire out of date information to ensure completeness and accuracy of the Knowledge Management Data Base (KMDB)	Report - Each SMP the number and type of new Knowledge artefacts produced, ones retired and updated, cross referenced to numbers of problems opened and closed and number of relevant changes introduced	-	SIAM 15	S
30	The Contractor shall provide to the Service Desk any information required to assist the Service Desk in the development, maintenance and continuous improvement of the end-user self-help facility	-	-	SIAM 16	S
Problem Management					
31	The Contractor shall comply with the Authority's Problem Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Problem Management Policies & Procedures as agreed during the on-boarding process. Example 1- provide root cause analysis document for all problem records raised within 24 hours. Example 2 – 99% of all problems raised to be investigated and closed within six months. To be agreed in the acceptance criteria.	-	SIAM 35	S
Release Management					
32	The Contractor shall comply with the Authority's Release Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Release Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 54	S

33	The Contractor shall minimise disruption to the Services through synchronisation of releases within packages	-	-	SIAM 56	S
34	The Contractor shall assist the Authority in the rapid delivery of change activity by providing a highly flexible and responsive Contractor release management process	-	-	SIAM 58	C
35	The Contractor shall deliver Releases into production in accordance with the relevant Project Plans	-	-	SIAM 59	C
Security Management					
36	The Contractor shall comply with the Authority's Security Policies and Procedures as referenced in Schedule R	Adherence to the relevant Service Request Policies & Procedures as agreed during the on-boarding process.	-	SEC 001	M
37	The Contractor shall support the security assurance audit contractor and the Authority to organise and complete audits. This includes but is not limited to: a. providing access to all relevant resources such as, staff with sufficient knowledge of the subject matter of the audit, contractor premises and relevant information; b. liaising directly with the security assurance audit contractor to try to agree factual accuracy of non-compliances and observations. Agreement shall not be unreasonably withheld by the Contractor. A clear explanation must be provided to the security assurance audit Contractor for any non-agreement; c. providing remedial actions with owners and completion dates to the Authority for each non-compliance that is agreed not more than 10 working days following the agreement of factual	-	-	SEC 002	M

	accuracy				
38	The Contractor shall attain and maintain security accreditation for all systems, services and applications under the Contractor's control	-	-	SEC 003	M
39	The Contractor shall support the security assurance vulnerability Contractor and Authority to organise and complete vulnerability scans. This includes but is not limited to: a. providing all relevant resources such as physical and logical access to systems and networks, change procedures, relevant information and key contacts; b. providing an initial impact assessment within 1 working day for those vulnerabilities deemed critical by the Authority and within 5 working days for all other vulnerabilities identified; c. taking the necessary action, as agreed with the Authority, to remediate vulnerabilities, unless agreed by the Authority that the vulnerability shall not be remediated	-	-	SEC 004	M
40	The Contractor shall support the Authority regarding Security Incident Management. This includes but is not limited to: a. providing all resources, information and access required by the Authority, or any third party appointed by the Authority to complete the investigation; b. establishing an effective security incident process and reporting mechanism; c. as security incidents occur, the Contractor shall report immediately to the Authority via the agreed	-	-	SEC 005	M

	security incident process				
41	The Contractor shall support the Authority regarding forensic investigations. This includes but is not limited to: a. providing all relevant resources such as physical and logical Access to systems and networks, information and key contacts; b. physically securing or seizing equipment identified as evidence in a forensic investigation in such a way as to preserve its integrity in line with best practice	-	-	SEC 006	M
42	The Contractor shall support the IT health check Contractor and Authority to organise and complete IT health checks and Penetration Tests. This includes but is not limited to: a. providing all relevant resources such as physical and logical access, change procedures, relevant information and key contacts; b. liaising with the Authority and the IT health check Contractor to agree factual accuracy of findings; c. providing an initial impact assessment within one business day for those vulnerabilities deemed critical by the Authority and within 5 working days for all other vulnerabilities identified; d. taking the necessary action, as agreed with the Authority, to remediate vulnerabilities, unless agreed by the Authority that the vulnerability shall not be remediated	-	-	SEC 007	M

43	The Contractor shall support external subject matter experts and consultants representing the Authority by providing reasonable and relevant information to the external party in a timely manner.	-	-	SEC 008	M
44	The Contractor shall ensure that all Contractor Staff (including any Sub-contractors|) receive appropriate information security training when joining the Contractor organisation. This includes but is not limited to: a. ensuring training is refreshed on an annual basis, maintaining the level of understanding of staff; b. where appropriate include security awareness material supplied by the Authority or authorised contractor(s); c. supporting the Authority or authorised contractor(s) in the production -of security awareness material specific to the Services	-	-	SEC 009	M
45	On receipt of security alerts or notices from the Authority, the Contractor shall respond to the Authority within agreed timescales detailing: a. actions already taken to mitigate the risk of such alert; b. actions that will be taken to mitigate the risk of such alert and timescales; or	-	-	SEC 010	M

	c. reasons why such alert poses no risk to the Authority				
46	The Contractor shall take steps to identify all situations which pose possible or actual threats or vulnerabilities to the confidentiality, integrity and availability of systems, process, data and people affecting the Authority relating to the Services provided by the Contractor. This includes but is not limited to: a. Creating and maintaining a register of identified threats and vulnerabilities. Detailed information about all threats and vulnerabilities must be reported to the Authority on a register determined by the Authority. Information in such register must include but not be limited to: *details of the nature of each threat/vulnerability *details of the source of each threat/vulnerability *an assessment of the severity of each threat/vulnerability to the Authority; b. Supporting the Authority's analysis of reported security threats/vulnerabilities by providing additional, complete and accurate information, as and when requested, including but not limited to: *information to inform the Authority's analysis of the threats/vulnerabilities; *information to help the Authority to assess the viability and cost of potential remedial actions c. Ensuring threats/vulnerabilities are managed effectively by monitoring and investigating them, raising a security	-	-	SEC 011	M

	incident when appropriate and documenting the issue; d. Following the identification of any threats/vulnerabilities, take such steps, in conjunction with the Authority, to implement resolutions and/or mitigations agreed by the Authority within agreed timescales e. Providing updates on agreed implementation of resolutions/mitigations to the Authority on a register determined by the Authority. This includes but is not limited to: *The current status of such implementation *Confirmation that the resolution/mitigation has been implemented *Details of issues preventing or delaying the resolution/mitigation from being implemented *Revised dates for implementation where appropriate				
47	The Contractor shall support the Authority's Protective Monitoring Service. This includes but is not limited to: a. Providing a formal documented route, or routes, for the Security Operations Centre to raise standard and major security incidents, and track to closure; b. Providing a formal documented route, or routes, for the Security Operations Centre to raise non-security incidents, and track to closure - e.g. non-delivery of system logs, connectivity or performance issues etc.; c. Agreeing security incident classification and prioritisation levels, along with associated SLAs, with the Security Operations Centre; d. Providing an interface for	-	-	SEC 012	M

	the Security Operations Centre and internal security functions to track the security incidents relevant to the SOC; e. Supporting & actively feeding security incident investigation updates into the Security Operations Centre, to allow them to track and close incidents on their internal incident management system; f. Supporting & raising security incidents into the Security Operations Centre, for action or situational awareness				
48	The Contractor shall support the Authority's Protective Monitoring Service by sharing information such as threat intelligence, vulnerabilities and less structured information, such as lessons learned reports, with the Security Operations Centre for situational awareness and tuning	-	-	SEC 013	M
49	The Contractor shall support the Authority's Protective Monitoring Service by agreeing a formal methodology and any necessary templates, for Management Information (MI)I/KPI reporting by the Security Operation Centre	-	-	SEC 014	M
50	The Contractor shall support the Authority's Protective Monitoring Service by mediating requests: a. to change devices to be monitored by the Security Operations Centre - e.g. on-boarding new devices, system migrations etc.; b. for Security Operations Centre data extracts, e.g. to support an investigation / forensics or for off boarding	-	-	SEC 015	M

51	The Contractor shall support the Authority's Protective Monitoring Service by establishing a Service Desk/Portal to: a. protect security incident related data appropriate to its BIL (IL2/Official), in storage and in transit; b. compartmentalise security incident related data (delegated management), providing access on a need to know basis; c. authenticate user access to security incident related data appropriately	-	-	SEC 016	M
52	The Contractor shall support the Authority's Protective Monitoring Service by providing an accurate assessment of Resource Unit Forecasts, to meet the capacity needs of the Authority against Quarterly Business Forecasts	-	-	SEC 017	M
53	The Contractor shall support the Authority's Protective Monitoring Service by Identifying, recording, investigating, diagnosing and resolving Problems assigned to them by the SOC Contractor in accordance with the relevant Service Levels and Key Performance Indicators	-	-	SEC 018	M
54	The Contractor shall support the Authority's Protective Monitoring Service by providing the relevant Management Information. This includes but is not limited to: a. Providing MI regarding attempted intrusions to the Authority, at a frequency and in a form to be agreed with the Authority; b. Provide a SMP, quarterly and annual report showing, but not limited to: *The number of new Security Cases by severity; *The number of open Security Cases by severity; *The number of Security	-	-	SEC 019	M

	Cases closed in the last period; *Broader trends observed within the Service; *A representation of the time to close each Security Case; *A representation of the time taken to "take action"; *The number of incidents which the "play book" was used and where it was proven effective; c. Capability to export/save reports in industry standard open formats including but not limited to CSV, PDF, HTML, XML				
55	The Contractor shall work in compliance with an information security management framework such as ISO 27001	-	-	SEC 020	M
56	The Contractor shall comply with all relevant legislation in terms of both operating and processing data on behalf of the Authority	-	-	SEC 021	M
57	The Contractor shall adhere to Home Office Security Policies, Standards and Processes, ensuring that any non-compliances are reported appropriately	-	-	SEC 022	M
58	The Contractor shall Identify, document and review audit trails for systems which Authority data is processed on, and inform the Security Expert Provider of any unusual or anomalous activity identified	-	-	SEC 023	M
59	The Contractor shall provide covert access to IT systems and data belonging to the Authority as requested by the Department	-	-	SEC 024	M
60	The Contractor shall implement or utilise an existing means of providing accurate time in logs and synchronisation between system components with a view to facilitating collation of events between those components (Network Technology Solutions NTS)	-	-	SEC 025	M
61	The Contractor shall take appropriate measures to secure both the internal and external boundaries of the	-	This GSO is applicable when a system	SEC 026	M

	system/solution provided to the Authority by the Contractor, this may include but not be limited to, IDS, IPS, Firewalls and DLP		(solution) is provided by the Contractor		
62	The Contractor shall provide Security Management Information and KPI reports as agreed upon within agreed timescales. The provision of Security Management Information could include statistics on but not limited to: a. Security Incidents; b. Security Awareness; c. Privileged Users d. Offshore Requests e. Audit Programme f. Clearance of staff such as Security Clearance, BPSS etc.	-	-	SEC 027	M
63	The Contractor shall obtain Cyber Essentials Certification to mitigate the risk from common Internet based threats	-	-	SEC 028	M
64	The Contractor shall ensure on-going compliance with all current and future security contractual obligations with which the Contractor must comply by: a. providing evidence to the Authority on a scheduled basis to demonstrate compliance; b. creating a corrective action plan to address identified areas of non-compliance and send the corrective action plan to the Authority for approval. Such corrective action plan must include but is not limited to: *Actions to be taken to rectify the non-compliance *Timescales for such actions *Owners of such actions	-	-	SEC 029	M

Service Design					
65	The Contractor shall provide the optimum amount of test environment resource to meet the Authority's business needs, re-allocating resource where possible and practical	-	-	SIAM 115	
Service Desk					
66	The Contractor shall comply with the Authority's Service Desk Policies and Procedures as referenced in Schedule R	Adherence to the relevant Service Desk Policies & Procedures as agreed during the on-boarding process.	-	SIAM 01	S
67	The Contractor shall assist the Service Desk to maximise Systems and Service Availability, performance and quality throughout the Contract Term.	KPI - Incident Acceptance & Handling (meaningful update) Severity 1 – every 30 minutes Severity 2 – every hour Severity 3 – once per day Severity 4 – once per day	-	SIAM 05	S
Service Level Management					
68	The Contractor shall comply with the Authority's Service Level Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Service Level Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 71	S
69	The Contractor shall achieve all required Service Levels and KPIs each SMP and provide accurate supporting documentation to the Authority to evidence this	- Monthly Service Reporting (or SMP), to be agreed during Service Acceptance The supplier Should provide a service report every month & meet monthly / quarterly depending on quality of service provided. These meetings will be at HO sites with any travel costs absorbed by the supplier.	-	SIAM 72	S
70	The Contractor shall resolve any failures to meet Service Levels	KPI **-** resolve all actions identified as part of the RAP/CAP Process within 3 SMPs or sooner	-	SIAM 73	S
71	The Contractor shall review Service Levels on an on-going basis and make recommendations to ensure the services continue to meet the Authority's business needs	-	-	SIAM 74	C

72	The Contractor shall prior to any new or changed service going live provide SIAM with an Operational Implementation Plan that meets the agreed quality standards and allows the service to be accurately measured	KPI - No of Contractor Services that have been introduced into live with an approved OIP target 98% (If the quality of the OIP is not up to standard then this would remain outstanding and not count as a success until it has been signed off/implemented)	-	SIAM 76	S
Standards and Architecture					
73	The Contractor will shall comply with the Authority's Standards & Architecture Policies and Procedures as referenced in Schedule R	Adherence to the relevant Standards & Architecture Policies & Procedures as agreed during the on-boarding process.	-	SIAM 116	S
74	The Contractor shall provide impact assessment to new Policies and Procedures and changes to existing Policies and Procedures within required timescales			SIAM 117	S
Supplier Management					
75	The Contractor shall comply with the Authority's Supplier Management Policies and Procedures as referenced in Schedule R	Adherence to the relevant Supplier Management Policies & Procedures as agreed during the on-boarding process.	-	SIAM 96	C
76	The Contractor shall undertake all activities required to ensure rapid on-boarding to the Authority's Service Management Policies and Procedures	-	-	SIAM 97	S
77	The Contractor shall provide an accurate and robust and regularly tested Exit Management Plan	-	-	SIAM 98	S
78	The Contractor shall resolve all Policies and Procedures non-compliances as soon as possible but no later than 3 reporting periods after the non-compliance has been raised	Report to show position with non-compliance, expected 80% resolved in 1 SMP 90% resolved in 2 SMP 100% resolved in 3 SMP escalation to Contract Management Board if fail clear non-compliance after 3 reporting periods	-	SIAM 99	S

Tooling (BAU)					
79	The Contractor shall comply with the SIAM Interface and Integration Requirements if interfacing with the Authority's IT Service Management Toolset (as per Tooling Requirements)	Compliance with the Authority's IT Service Management Toolset Integration Requirements	The Authority will deploy technology to provide all the integration points to which the Contractor will be required to connect The levels of integration will be agreed with the Authority and will take into account data volumes, rates and patterns. Automated integration will be achieved through strategic industry standard protocols The level of configuration at the point of integration will be minimal with standard fields used for data mapping The Authority will provide the Contractor with a Tooling Interface Requirements document to enable Suppliers to Interface with the Authority's IT Service	SIAM 118	

			Management Toolset		
Availability and Performance Monitoring					
80	The Contractor shall provide an automated integrated feed for availability and performance data from the Contractors system tool(s) into the Authority's IT Service Management toolset. .	The desired outcome is that the Authority has the visibility of system and service impacting events in a timely and transparent manner	-	TI8	S
81	Tooling interface will be one-way with performance and availability data being sent from the Contractors management system in near real time (or real time depending on commercial viability)	-	-	TI9	S
Security Events					
82	The Contractor shall provide an automated integrated feed for filtered security events from Contractors system tool(s) into the Authority's Security Operations Centre (SOC)	-	-	TI19	S
83	An automated integrated feed will be established by the Authority for filtered security events from the Authority's Security Operations Centre (SOC) to the Authority's IT Service Management Toolset	-	-	TI20	S
84	The security events interfaces will be 1-way with events being sent in near real time (or real time depending on commercial viability)	-	-	TI21	S
85	A draft 'Security Event filtering and Correlation Rules Specification' will be defined by the Authority with input from the Contractor. This specification will include but not limited to the security events that will be passed into the Authority Security Operations Centre, 1st and 2nd level correlation rules, security event types, category, frequency and expected volume	-	The draft specification will be subject to joint review and amendments as required before sign-off by Authority. The Authority will provide final confirmation on what	TI22	S

			security events are to be provided. This specification will be maintained by the Authority and held on the ITSM Knowledge Management system and will be property of the Authority		
86	After go-live the Authority will hold review meetings with the Contractor on the filtered security events being passed. The Authority reserves the right to request changes, if required, for a period of up to 6 SMP after go-live (known as Tuning Phase). All changes in this period shall be subject to the Change Control Procedure.	The desired outcome is that the Authority has the visibility of security events in a timely and transparent manner	These reviews will start in the 2nd SMP period and be held weekly for the first SMP; moving to once each SMP thereafter. The purpose of the reviews is to tune the service to ensure it meets the Authority's desired outcome	TI23	S
Vulnerability Scanning					
87	The Contractor shall provide an automated integrated feed for providing Vulnerability Scanning data from the Contractors estate into the Authority's Security Operations Centre (SOC)	-	-	TI24	S
88	An automated integrated feed will be established by the Authority for this data from the Authority's Security Operations Centre (SOC) to the Authority's IT Service Management Toolset	-	-	TI25	S
89	The interface will be 2-way: The Authority's vulnerability scanning tool within its SOC will initiate scans for known vulnerabilities in the Contractors IT estate, scanning an agreed number of devices, per agreed period	-	-	TI26	S

	The tool will return its findings to the Authority's SOC in near real time to an agreed operational level				
90	A draft 'Vulnerability Scanning Data' specification will be defined by the Authority with input from the Contractor. This specification will include but not limited to: Description of in scope assets extracted from the Contractor provided asset data; Specifying the data format, frequency and expected volume of scanning reports to be returned to the Authority's Security Operations Centre	-	The draft specification will be subject to joint review and amendments as required before sign-off by Authority. The Authority will provide final confirmation on what known vulnerabilities are to be scanned for and the frequency that scans are to be provided. This specification will be maintained by the Authority and held on the ITSM Knowledge Management system and will be property of the Authority. The Authority will work with the Contractor in the identification and frequency of assets to be scanned.	TI27	S
91	Following go-live the Authority will hold review meetings with the Contractor on the Vulnerability Scan data being passed. The Authority reserves the right to request changes, if required, for a period of up to 6 SMPs after go-live (known as Tuning Phase). All changes in this period shall be subject to the Change Control procedure	The desired outcome is for an interface that will provide automated information that can be used by the Authority to maintain up to date security information about Service Assets required to deliver a the Authority's IT Service, in timely and transparent manner	These reviews will start in the 2nd SMP period and be held weekly for the first SMP; moving to once each month thereafter. The purpose of the reviews is to tune the	TI28	S

			service to ensure it meets the Authority's desired outcome		

Please refer to Appendix C for Balanced Scorecard Measures

4. APPENDIX A – MESSAGING AND DATA FLOW

This appendix provides an overview of the information to be communicated between The Home Office, the Travel Service Provider and the Escort Service Provider with relation to immigration enforcement travel and escorting. The focus is on the data being sent in and out of The Home Office, there is no consideration to the different departments within the Home Office, also some of the information is critical to the business processes, others just for MI; both categories of information are included here without distinction.

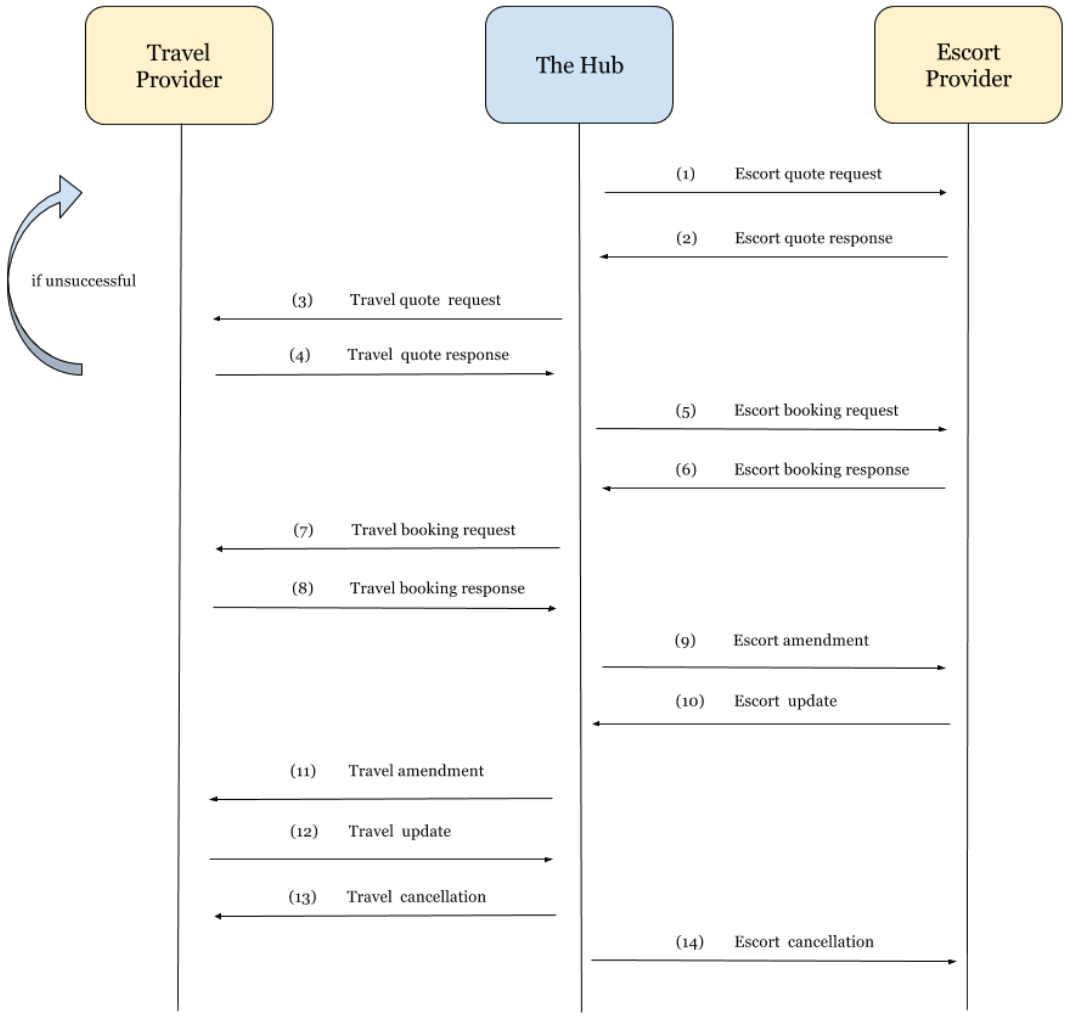
The process of arranging the logistics to deport a returnee is to be arranged through the passing of information in the following sequence.

The information can be sent to the Home office manually, through a Home Office supplied portal or directly from the TSP system though an API or structured data message protocol.

Much of the data exchange is between the two providers. The Home reserves the right to access communication between the TSP and the ESP.

The information expressed here is expressed in a reasonably structured form to enable a TSP to understand how they would be able to technically integrate to the Home Office.

The data messages shown below are for illustrative purposes only. The Service Provider IT system must be able to handle this information; the full list of messages will be finalised during mobilisation.



4.1 Message 1: Escort quote request

A request sent from the Home Office case worker to the Escort Service Provider. The case worker has reviewed some information internally and then triggered this request to start the process of removing someone from the UK.

It is anticipated that for an escorted removal the greatest constraint will be the Escort Service Provider's availability so they are to be contacted first.

Purpose

Home Office providing detail of a removal for the Escort Service Provider to respond as to which they can fulfil.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Personal Details	Personal, static information about the returnee. Note there could be more than one.	HO returnee reference, Name, Date of Birth, medical conditions e.g. blind, wheelchair.
Escort risk assessment	A set of variable attributes for each returnee has that the Escort Service Provider needs to decide their response. Note this is likely to be more than what was passed to the Travel Service Provider but still only what is needed for this purpose will be passed, not the full set of risk information held by the Home Office.	Violent, disruptive, sexual offender.
Returnee Location	Where the returnee is most likely to be at the time of their departure, so the Travel company can consider local airports. Note this is per returnee, it is possible, but unlikely that a family group is split up in the detention estate but will fly home together.	Detention centre ID, Prison ID, specific address.
International	Is it an international or in country move.	International indicator.
Escort on Transport	It is possible that in some low risk scenarios that the returnee is taken to the transport vehicle (Plane) but the escorts leave them at the gate and wait for the transport to leave before returning home.	Escort needed on transport indicator.
Dates	A range of dates that we'd like the Returnee(s) to travel over.	Earliest leave date, latest Leave date, exclusion dates.

4.2 Message 2: Escort quote response

The Escort Service Provider will respond to an escort request with their risk evaluation as to how many Escorts they believe are needed, and any supplementary people, such as medics etc.

The Escort Service Provider is to identify multiple options (across different days) that they can support. The greater the options provided by the Escort Service Provider then the greater the possibility of the Travel Service Provider finding a cheaper overall removal cost.

Purpose

The Escort Service Provider giving their details as to what they would do, at what effort, giving multiple options

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Escort quote ID	For each escort quote there is to be an escort quote ID, because the risk profile can change the escort quote may change for the same travel request so this needs to be separate.	Escort quote reference
Escort Date	The date for which the escort quote reference are valid for.	Date
Escort Info	The number of escorts and the type. Some Returnees require medics and the Escort Service Provider may have multiple categories of escort based on gender, physique, language. This is a function of the returnee and as such is expected to be common to all quotes.	Escort number Escort type
Escort Segment	The escorting may require multiple journeys which vary based on means of transport, whether the returnee is present and potentially the escorts (involving a hand over between teams). This is a function of the route and as such is expected to be common to all quotes.	Segment ID, Start point finish point, transport type
Escort Effort	Per segment per escort there is a cost or a time duration. This is a function of the route and as such is expected to be common to all quotes.	Cost / time
Escort details	Per Quote, Per segment of the escort quote the names of the escorts and the vehicle ID are needed. At some point the advanced passenger information is needed and if it is available now then it could be provided – but not mandatory, could	Segment ID, escort Name

	be sent later.	

4.3 Message 3: Travel quote request

A request sent to the Travel Service Provider about what travel is needed and for who.

For unescorted flights the workflow starts here. In this case the “travel Details” will be specified by The Home Office user.

For escorted flights this information is sourced from the Escort Service Provider and either comes direct from them or via the Home Office.

Purpose

Home Office providing detail of a removal for the Travel Service Provider to find quotes.

Data Set	Description	Example
Travel request Identifier	Unique reference for the request.	Removal reference
Personal Details	Personal, static information about the returnee. Note there could be more than one.	HO returnee ID, Name, Date of Birth, noted conditions such as: blind, wheelchair etc
Travel Document	The type of document each returnee has to enable them to travel.	Passport, National identity card, Emergency Travel Document.
Travel risk assessment	A set of variable attributes for each returnee has that the airlines are interested in and may refuse travel based upon. Note only what is needed for this purpose will be passed, not the full set of risk information held by the Home Office. The security level of the travel company is not high, so this is likely to only be a small set of the risk information.	Violent, disruptive, number of escorts.
Returnee Location	Where the returnee is most likely to be at the time of their departure, so the Travel company can consider local airports.	Detention centre ID, Prison ID, specific address.
Escort Dates	The dates returned by the Escort Service Provider.	Date 1, 2, 3
Destination	Where the returnee(s) is to go.	Free text location
Constraints	The constraints concerning for travel are contained within the TIG.	Refundable, airline exclusions, cost limit

4.4 Message 4: Travel quote response

The Travel Service Provider’s response to a travel request, giving a number of possible options for each of the Escort Service Provider’s dates for the Home Office to choose from.

Purpose

Travel Service Provider provides a list of travel quotes for each of the Escort Service Provider's declared available dates back to The Home Office with travel details and associated costs.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Escort Quote reference	To match the travel quotes to the Escort quotes.	Escort quote reference
Travel Quote reference	Unique reference for each of the quotes in the response.	Travel quote reference
Travel Cost	For each quote there will be a cost per traveller and a total.	Cost for returnee 1, cost for escort 1, total cost, currency
Travel itinerary	Each quote will break into one or more segments, each segment will have start and end times and locations, Ref Ids, carrier ID, and segment type.	Dates, times, flight numbers, provider name (British airways, Marriott…), segment type (plane, ferry etc)
Travel Conditions	Covers specific information applicable to this quote, maybe it expires quickly, or is non-refundable etc.	Non Refundable, hand baggage only fare

4.5 Message 5: Escort booking request

The Home Office will receive the Travel Service Provider's quote response and will first assess if the information about the returnee is the same as it was when the quotes were sourced. The behaviour of the returnee may have impacted their risk profile requiring a re-quote from either or both providers. In these cases the workflow returns to message 1.

If the information is unchanged the Home office will choose their preferred quote and then give the Authority to book.

Purpose

The message from The Home Office to the Escort Service Provider requesting to book against one of their previously provided quotes.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Escort quote reference	To be clear which quote we want to book.	Escort quote reference
Book	Booking command.	Book

4.6 Message 6: Escort confirmation response

The Escort Service Provider will respond to the booking request with the names and as much other information as they can at this point related to their people and vehicles.

Purpose

Message from the Escort Service Provider to confirm a booking and provide the names of the escorts, or when it can't be confirmed then why.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Escort quote reference	To be clear which quote HO are referring to.	Escort quote reference
Accepted	Simple confirmation that the booking has been made.	Confirmed

4.7 Message 7: Travel booking request

The Escort Service Provider confirm their escort arrangements after the Home office has chosen their preferred option, if one of the TSP quotes is chosen, then the Home Office will request the TSP to book travel. It means that the Travel booking request may be sent at the same time as the Escort booking request.

Purpose

Message from The Home Office to the Travel Service Provider to book one of their previously issued quotes.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Travel quote ID	To be clear which quote HO want to book.	Travel quote reference
Book	Booking command.	Book
Escort details	To book the tickets for the Escorts the Travel company needs their names (mandatory) and their advanced passenger info (non mandatory at this point.	Escort 1 name, escort 1 passport number, escort 1 flight meal = Vegetarian

4.8 Message 8: Travel booking response

The response to a confirmation request from the Travel provider is very similar to the Escort response, including the cancellation options. The difference here is that the Home Office is expecting back the travel documents

Purpose

Message from the Travel Service Provider to confirm a booking and provide the names of the escorts, or when it can't be confirmed then why.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference

Travel quote reference	To be clear which quote HO are referring to.	Travel quote reference
Accepted	The Travel Service Provider need the ability to decline a booking request. In the instance where they could, but no longer can, deliver against the travel quote request, they need to reply, “declined”.	Booked Declined
Decline Reason	One of a list of predefined options, (that realistically will be modified over time).	Suggested options they could choose from: flight cancelled,
Decline details	A fuller reason for the decline, free text fields are hard to report from, hence why HO have the decline reason to support this.	Free text
Travel confirmation details	We are going to expect the Travel Service Provider to send the details of what has been booked, ticket numbers etc. These may be details typed into the travel system by their staff, they may be attachments, images, pdfs of etickets too, currently unknown as to how this would work.	eTickets, booking id. Ticket numbers

4.9 Message 9: Escort amendment

There are many things that can change between the booking being confirmed and the commencement of the removal. The returnee’s location could change, their risk profile might change. The Home Office needs to inform the Escort Service Provider so they can take action. Most of these changes will trigger an update from the Escort Service Provider to inform the Home office of the consequence of their request

Purpose

Message from The Home Office to the Escort Service Provider to inform them of a request to change a confirmed booking.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Escort quote reference	To be clear which quote HO are referring to.	Escort quote reference
Escort request details	The segments that are affected need to be identified and then the new .detail specified. It could be that a segment is cancelled, or that two segments are to be replaced with one new one.	Segment ID, locations, times Whether something cancelled
Other	To cover scenarios out of scope there may need to be a catch all free text box.	Free text

4.10 Message 10: Escort update

The Escort update message is a catch all exception management tool. HO do not currently anticipate an update from the Escort Service Provider in the successful path flow where the flight has departed without incident. However if something has changed in the Escort Service Provider domain then this update is needed to inform The Home Office.

The change could be before the Escort team has departed, could be while the Escorts are moving the returnee, and could be while at the airport. Might even be while they are in the air in case of a diversion.

Because some of the escort details are not needed for flight booking but are needed for travel, like passport number, this message can be used to provide this later data.

Purpose

This is a flexible message from the Escort Service Provider that indicates either the escorting was completed, or if not then the current status of the situation.
The message is also to be used to advise The Home Office of any changes to (or new) information about the escorts.

The message is also to be used to advise The Home Office of the consequence of any amendment requests made by The Home Office.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Escort quote reference	To be clear which quote we are referring to.	Escort quote reference
Completed info	If the escort is completed successfully then The Home Office is to be informed with details.	Confirmed, Per segment, date time leave, date time arrive. Free text if needed
Cancellation	If the escorting is to be aborted for some reason then The Home Office is to be informed with reasons. If this has happened sufficiently far ahead of the flight then it might be possible to change the flight. With the tracking Information it may be possible to redirect the returnee to a point other than their starting location.	Cancellation, Reason, free text field if needed
Unsuccessful	If the escorting has started and has to abandon the escorting, could be because the returnee is disruptive or ill, or in sufficiently serious delay that the journey is to be aborted. This occurrence is likely to trigger the Home Office to cancel the corresponding Travel booking.	Unsuccessful, Reason, Free text field
Delayed	If the Escort is delayed, then the Escort Service Provider is to inform	Delay reason, affected segment ID , new start and

	the Home Office with details of where and their new itinerary - a delay to one segment may have knock on impacts to others. This may result in a change of flights, or the Home Office issuing a cancellation.	end times Free text field
Escort change	It could be that the Escort Service Provider needs to change the escort. This will almost certainly require a change of name on any flight ticket.	Per segment: Escort ID to be removed, Escort ID to be added

4.11 Message 11: Travel amendment

It is possible that The Home Office will want to modify a travel booking either to provide additional information that wasn't known earlier, such as a passport expiry date of an escort, or to change one piece of information held. Note some of this information is from the Escort Service Provider. This data exchange has been expressed as if the Home office is routing information from the ESP to the TSP. If the agreed approach has direct communication from the ESP to the TSP, then this amendment message may be sent from the ESP.

Some changes will be minor, such as the change of an Escort passport number, others will be more significant and may incur charges or even be not possible, such as a flight time / date change or a name change.

The Home Office expect that the majority of Travel amendments will trigger a Travel update message response.

Purpose

Message from The Home Office to the Travel Service Provider to inform them of a request to change a confirmed booking.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request	Removal reference
Escort quote reference	To be clear which quote HO are referring to.	Escort quote reference
Travel details update	The details of a confirmed booking that require adding or amending.	Passport numbers, expiry dates associated to passengers.
Flight details update	The details of an amendment to the itinerary, either passengers or routing.	Old affected itinerary section, new itinerary specifications.
Other	To cover scenarios out of scope there may need to be a catch all free text field.	Free text

4.12 Message 12: Travel update

The Travel update message is a catch all exception management tool. HO do not currently anticipate an update from the Travel Service Provider in the successful path flow where the flight has departed without incident. However, if something has changed in the Travel Service Provider domain, then this message is needed to inform The Home Office.

The change could be before the Escort has departed, could be while the Escort is moving the returnee, and could be while at the airport. Might even be while they are in the air in case of a diversion.

Purpose

Message from the Travel Service Provider to inform the Home Office of either something that has happened from their side or to respond to a post booking request from The Home Office.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Travel quote reference	To be clear which quote HO are referring to.	Travel quote reference
Completed info	An update of a successful flight, could include actual departure and arrival times – probably not necessary.	Confirmed, date time leave, date time arrive.
Flight Change	Should a flight be changed the Home Office will need to understand which flight and by how much. The change could be a formal change of time / terminal, or a delay.	Change reason, flight number. Old flight details, new flight details
Cancellation Details	Similar to a flight change, but more serious. To include which reference (probably all).	Cancellation reason, flight number. Old flight details,
Financial	For the Travel Service Provider to inform the Home Office of the financial consequence of their requested post booking changes.	Refund info, fee info (could be a change fee or cancellation fee) Reason field
Unknown other exceptions	The HO anticipate, that there will be other scenarios that haven't been considered yet. These may be managed though additional structured fields but there will always be a need to fall back to a free text field in emergencies.	Free text

4.13 Message 13: Travel cancellation

Simple cancellation. Potentially the HO may look to inform the Travel Service Provider that we wish to cancel the use of this flight for this booking, but reuse it – dependent on carrier T&Cs etc. The message structure is subject to change. Sending this is likely to trigger a Travel Update response with the financial consequences.

Purpose

The Home Office notifying the Travel Service Provider a flight is to be cancelled.

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request	Removal reference
Travel quote reference	To be clear which quote HO are referring to	Travel quote reference
Cancel	Simple cancel command	Cancel

4.14 Message 14: Escort cancellation

Simple cancellation.
Sending this could trigger an Escort Update response with the financial consequences.

Purpose

The Home Office notifying the Escort Service Provider an escort booking is to be cancelled

Data Set	Description	Example
Travel request Identifier	Reference for the Home office to match this to the initial request.	Removal reference
Escort quote reference	To be clear which quote HO are referring to.	Escort quote reference
Cancel	Simple cancel command.	Cancel

APPENDIX B – HUB REQUIREMENTS

The Hub is the case working tool that the Home Office will use to show the current status and information pertaining to a movement or removal case. The Hub will have a UI for the Home office users to key in the necessary fields. To enable the TSP to inform the Home Office of their information the Hub could integrate with supplier systems, conversely the Authority expects bidders for the TSP to articulate how they would provide the information required by the Authority whether via an integrated interface that will be built in to the service (please see Annex D) or a web form provided by the Home Office. Either of these options is to form part of the TSP bid submission.

4.15 Service Access (Authority System)

Access to the “Hub” will be from within the HO staff’s existing authentication suite

4.16 Roles and Responsibilities

With the hub there will be multiple user roles. The user role will determine the capabilities of the user with respect to their ability to view and edit any information related to the removal of a returnee. The hub will include functionality around the management of its user base facilitated through a service administrator user role

4.17 Travel Service business rule management

The constraints under which the Travel Service Provider is selecting travel quotes are aggregated into an Excel Spreadsheet (TIG). This will be available to the TSP and mutually maintained by the TSP and the Home Office.

The rules refer to dates travel can’t be booked on, carrier exclusions, immigration case quotas and route specific complications.

Some of the messages that the Home Office is expecting from the Travel Service Provider includes selections from predetermined lists, e.g. Cancellation reason. The list of options for each of these fields will be held in the hub. The system administrator role will have the ability to edit these lists of options which will prompt communication to the Travel Service Provider of the new data.

4.18 Travel Request service approach

Once the Home Office has made the decision to remove someone from the UK then their case owner will trigger the removals process from within the hub.

The removals process will start with the case worker accessing information and requesting to “remove”.

The hub will then perform some risk profiling using business logic against information available. This will determine if the removal is to take place with Escort/s or not and potentially whether the travel Service Provider will need to provide a ticket.

If escorting has been judged necessary, then a request will be made of the Escort Service Provider to give options as to when they can fulfil the request. Their response will also give their decision on number of escorts and support staff based on the information about the returnee that the Home Office has provided them.

The travel Service Provider will identify a number of quotes as defined in schedule D.

The Home office will make a judgement call as to which of the option to proceed with. If the chosen option is to proceed with one of the travel Service Provider quotes then the Home Office will inform the travel Service Provider to make a confirmed booking. (an alternative is to use a charter flight, the management of which is held within the Home Office)

4.19 Search Function

The hub will have some search capability available to some / all user roles. The search criteria will have aspects such as Case reference number and Returnee name.

The result of the search will enable a user to access a returnee case within the hub and view the activity.

It may be that some searches will exclude some cases based on user role and the “sensitivity” of the case.

4.20 Travel Amendments and Cancellations

The Home Office user will have the ability to trigger an amendment or cancellation request against a case to the Travel Service Provider. The Home office user may have to provide reasons. The travel Service Provider is to act on these requests promptly and respond with their confirmation and any consequences of the action – costs incurred etc.

4.21 Booking Status

All Home Office staff that have an interest in the case will have the ability to access the hub and have the availability to view the cases that are relevant to them. The relevant capabilities within the Home Office are to be notified of changes/progress of relevant cases. The notification approach has not been determined.

4.22 Duplicate bookings

The hub will not permit a user to request removal for a returnee if there is an existing booking. Every case will have a unique reference and for every case, every removal request will have a unique reference.

APPENDIX C

Balanced Scorecard Measures

Incident Management

Service Level - 99.5% (minimum) Incident Resolution Severity 1, Report down to Contractors Service/site level. Target time 4 hours of incident being assigned
KPI - 99.5% (minimum) Incident Resolution Severity 2, Report down to Contractors Service/site level. Target time of 8 hours of incident being assigned
KPI - 98% (minimum) Incident Resolution Severity 3, Report down to Contractors Service/site level. Target time of 2 working days of incident being assigned
KPI - 98% (minimum) Incident Resolution Severity 4, Report down to Contractors Service/site level. Target time of 4 working days of incident being assigned

Problem Management

Service Level - Problem Resolution Urgent Contractor Service Repairs. 95% Target
Service Level - Problem Resolution Non Urgent Contractor Service Repairs. 95% Target
Service Level - Repairs completed by the Contractor within an SMP which are not Faulty 95% Target

Change Management

KPI - % of changes that were successfully implemented without the need for rework each SMP. 99% Target

Release Management

Service Level - Contractor Service Software Releases, Security Releases and Anti-Virus (AV) Software Releases successfully installed within the applicable timescales within a SMP. 99% Target

IT Asset & Configuration

Service Level - % check of Configuration Items accurately recorded in the Configuration Management Database by means of a physical check of the percentage of a minimum of 500 Configuration Items (CI) per SMP including all associated software licence checks. Target 99%

Availability Management

KPI - Contractor Service Availability each SMP. 99.80% (minimum) Target
KPI - Contractor Service Reliability each SMP. 99.70% (minimum) Target

Capacity Management

KPI - No of instances caused by a lack of adequate IT capacity. Target no more than 1 instance per reporting period.

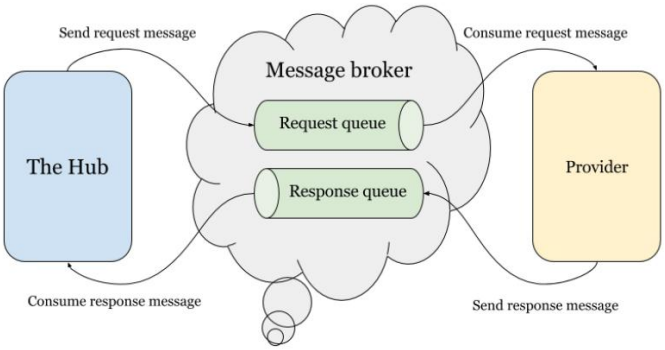
APPENDIX D

Travel and Escorting Interface Communication (ICD) Overview
This document describes the technical aspects of a potential interface between the Hub and both Travel and Escort Service Providers. The purpose of the Hub is to enable the Home Office to execute escorted and un-escorted out-of-country removals and in-country moves. In order to complete this task the Home Office needs to liaise with its Travel and Escort Service Providers.

High-level architecture
If the Hub were to be integrated with both Travel and Escort Providers then the Home Office suggests using a sequence of messages which will be exchanged over a message broker (which may be exposed to the providers via a restful API). Each message type would have its dedicated message queue and both providers will be able to access relevant message queues. The business meaning and semantics of each of the messages is described in a separate document. The exact syntax for each of the messages will be defined at a later stage.

Security
The Hub will use mutual SSL authentication. Both Travel and Escort Service Providers would each supply a signed certificate that would be used by the Hub to authorise access to the service. Access to specific message queues will be controlled by the Hub based on credentials supplied to the service. The Home Office uses a Single Sign-On solution to manage access to its applications. Providers will use GSS API (Generic Security Services API) to obtain an access token from the authentication service which will be used by the message broker to authorise users. User credentials will be on an organisational level for each provider.

Service Level Agreement duration
The duration of each of the SLAs will be counted from the moment a request message is put on a queue rather than from the moment it is consumed by a provider.

Error handling
For each message queue there will be an accompanying error message queue (named after its original queue <QUEUE>-error). The consumer of the original will write to the error message queue when it has problems processing the original message. The purpose of the error message queues is to deal with technical problems (i.e.: can not parse JSON message) while business related issues should be covered by exchange of other messages (i.e.: no flights available). Error messages should contain a unique id of the failed message (business id such as removalId), its time stamp and failure description.

Message format
The Home Office will provide examples for each of the messages as well as schemas describing data format. Messages sent by the Home Office and providers should be validated against the schema. The payload of all messages will be a structured JSON document.